

# **EXHIBIT 4**

UNITED STATES DISTRICT COURT  
  
**SOUTHERN DISTRICT OF NEW YORK**

SECURITIES AND EXCHANGE  
COMMISSION,

Plaintiff,

v.

SOLARWINDS CORP. AND TIMOTHY G.  
BROWN,

Defendants.

Civil Action No. 23-cv-9518-PAE

**REBUTTAL EXPERT REPORT OF MARK G. GRAFF  
JANUARY 24, 2025**

## TABLE OF CONTENTS

I.	INTRODUCTION AND ASSIGNMENT .....	1
II.	SUMMARY OF OPINIONS .....	3
III.	METHODOLOGY .....	5
A.	My Responses to Dr. Rattray’s Issues with My Methodology .....	6
B.	Dr. Rattray’s Methodology Was Flawed .....	9
1.	The analysis that Dr. Rattray undertook did not “approximate the methodology” of a cybersecurity assessment.....	9
2.	Dr. Rattray relied upon non-existent qualifying language in the Security Statement .....	11
IV.	ACCESS CONTROLS .....	13
A.	Dr. Rattray’s Analysis of SolarWinds Developers’ Access to Production Data Is Flawed.....	13
B.	Dr. Rattray’s Analysis of SolarWinds’ Exposure of the Password “solarwinds123” Is Flawed .....	16
C.	Dr. Rattray Incorrectly Argued that I Drew “Inferences from Isolated Notations in Documents” .....	17
D.	Dr. Rattray’s Dismissal of SolarWinds’ FedRAMP Assessment Is Unsupported.....	20
V.	PASSWORDS AND USER AUTHENTICATION .....	22
VI.	SOFTWARE DEVELOPMENT LIFECYCLE .....	27
A.	Dr. Rattray’s Statements Related to the Separation of Development and Production Environments Are Incorrect .....	27
B.	Dr. Rattray’s Statements Related to the Development of Internal Software Applications Are Flawed .....	30
C.	Dr. Rattray’s Statements Related to Threat Modeling and Security Testing Are Incorrect .....	33
VII.	DECLARATION .....	40

## I. INTRODUCTION AND ASSIGNMENT

1. My name is Mark G. Graff. My qualifications were covered in my original report in this matter, dated October 25, 2024 (“my Opening Report” or the “Graff Opening Report”).<sup>1</sup> That report summarizes my qualifications, provides background on SolarWinds and Tim Brown (together, “Defendants”), summarizes the SEC’s allegations in this matter, and describes the produced documents, deposition transcripts, and publicly available materials that I considered as of October 25, 2024.

2. In my Opening Report, I provided my analysis and opinions on a technical comparison between the state of SolarWinds’ cybersecurity depicted in (1) the Security Statement posted on its public website between 2017 and 2020 and (2) internal assessments, presentations, and communications regarding the state of cybersecurity during that same timeframe with respect to SolarWinds’ methods for access control, user authentication, and network monitoring, as well as its use of a secure development lifecycle and adherence to the NIST Cybersecurity Framework.<sup>2</sup> Based on my review and analysis, I concluded that, with respect to access control, user authentication, and secure development lifecycle processes, there were significant discrepancies between the cybersecurity practices SolarWinds claimed to be performing in the very broad, categorical, and unqualified assertions in the Security Statement and the cybersecurity practices I have observed from its internal assessments, presentations, and communications. Based on these internal SolarWinds documents, I also concluded that significant deficiencies within these areas were known or made known to the relevant

---

<sup>1</sup> Expert Report of Mark G. Graff, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 25, 2024 (“Graff Opening Report”).

<sup>2</sup> Graff Opening Report, ¶ 17.

cybersecurity and leadership personnel.<sup>3</sup> Finally, I concluded that the fact that elementary cybersecurity issues slipped through the company's internal systems should have alerted SolarWinds' cybersecurity leadership that the Security Statement was inaccurately describing SolarWinds' cybersecurity posture.<sup>4</sup>

3. On November 22, 2024, Defendants submitted a report by Dr. Gregory Rattray (the "Rattray Report").<sup>5</sup> Counsel for Plaintiff has asked me to review and respond to the Rattray Report based upon my expertise. In this rebuttal report I respond to particular points on which I disagree with Dr. Rattray. The fact that I do not respond to others does not mean I agree with or concede his points.

4. In working on this assignment, I considered the documents listed in **Appendix C** of my Opening Report. Some additional documents were provided by opposing counsel after I submitted my Opening Report. Of those additional documents, the ones I considered are listed in **Rebuttal Appendix A** of this report. My work on this matter is ongoing, and I reserve the right to supplement my analysis and opinions as more information becomes available to me.

5. My hourly rate for work on this matter is \$1,000. Some of the work underlying the conclusions of my expert report was performed under my direction and guidance by employees at Analysis Group, Inc., an economic and litigation consulting firm. Neither my compensation nor that of Analysis Group, Inc., is contingent upon my findings, the testimony I may give, or the outcome of this litigation.

---

<sup>3</sup> By "relevant cybersecurity and leadership personnel" at SolarWinds, I refer to the SolarWinds employees described in Table 1 of the Graff Opening Report.

<sup>4</sup> Graff Opening Report, ¶¶ 20-28.

<sup>5</sup> Expert Report of Gregory Rattray, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, November 22, 2024 ("Rattray Report").

## II. SUMMARY OF OPINIONS

6. Overall, I conclude that Dr. Rattray’s criticisms of my expert report are based on inaccurate characterizations of my report’s opinions and content. Further, Dr. Rattray’s report is methodologically flawed and is therefore unreliable. Thus, none of Dr. Rattray’s opinions have changed the opinions in my Opening Report.

7. As I explain in **Section III.A**, Dr. Rattray’s characterization of my assignment, analyses, and findings is inaccurate; thus, his criticisms of my methodology are invalid. He asserted that my methodology was not a “standard cybersecurity assessment,” ignoring that my assignment was not to conduct such an assessment. My methodology of reviewing SolarWinds’ internal documents and emails was in line with my assignment to compare the state of SolarWinds’ cybersecurity depicted in the Security Statement and internal assessments, presentations, and communications regarding the state of cybersecurity.<sup>6</sup> His opinion that I drew conclusions about the frequency of cybersecurity issues based on isolated incidents ignores that the gravity of these incidents indicates a systemic issue. Dr. Rattray’s unsupported assertion that these were “not events of significant magnitude” is directly contradicted by contemporaneous internal communications from senior SolarWinds employees.

8. In **Section III.B**, I explain why Dr. Rattray’s methodology—a self-described “approximation” of a cybersecurity assessment—is flawed and is therefore unreliable. He assessed in many cases whether a policy *was in place*, but did not reliably evaluate whether the policies were *implemented* in line with the Security Statement and industry custom and practice.

---

<sup>6</sup> Graff Opening Report, ¶ 17.

Additionally, Dr. Rattray's analysis improperly relied upon qualifying language on multiple occasions, that does not, in fact, exist in the Security Statement.

9. In **Section IV**, I explain how Dr. Rattray failed to support his arguments that the incidents I analyzed related to access controls were "one-off issues with marginal if any relevance." He did not dispute that the events I cited occurred. Instead, he merely argued that they were "isolated"—a characterization that is speculative and unsupported by the evidence. Additionally, Dr. Rattray's dismissal of the SolarWinds FedRAMP assessment as a "budgeting exercise—not a security exercise," ignored the valuable information it contained about the state of SolarWinds' cybersecurity controls.

10. In **Section V**, I describe why Dr. Rattray's attacks of my opinions regarding the Security Statement's assertions related to passwords are misguided. Contrary to Dr. Rattray's suggestions, it is irrelevant that SolarWinds did not have a "general policy or practice of allowing accounts to be shared," or that hard-coding passwords in configuration files was not "allowed." Once again, the problem was the practices on the ground. The use of shared accounts and existence of weak passwords for sensitive systems indicate that SolarWinds lacked the capability to ensure that (or even to monitor whether) its policies were implemented, in contrast to the assertions in the Security Statement.

11. In **Section VI**, I describe why Dr. Rattray was incorrect in opining that my Opening Report did not show any systemic failure to follow the Software Development Lifecycle ("SDL"). First, contradicting the opinion of a senior SolarWinds employee, Dr. Rattray minimized the significance of an incident involving the lack of separation between development and production environments. Dr. Rattray did not dispute in his report that development occurred in the production environment during the Relevant Period, and instead quibbled over which part

of the Security Statement this poor practice contradicted. Second, Dr. Rattray failed to recognize that the Security Statement’s assertion that “all development activities” follow best practices includes internal software applications. Third, Dr. Rattray’s description of threat modeling as “a loose term that can encompass virtually any effort” is not in line with the best practices described by leading industry bodies, including the Open Worldwide Application Security Project (“OWASP”), NIST, and Microsoft.<sup>7</sup> Dr. Rattray failed to present evidence showing that SolarWinds consistently engaged in threat modeling, which is a standard security practice within a secure development lifecycle, and would have been a fundamental element of the “security best practices” mandated by the company “across all development activities,” as claimed in the Security Statement.

### III. METHODOLOGY

12. Dr. Rattray asserts that he has identified several problems with my methodology.<sup>8</sup> However, as I show in **Section III.A**, Dr. Rattray’s characterization of my assignment, analyses, and findings is inaccurate—thus, his criticisms of my methodology are irrelevant.

13. Additionally, as I show in **Section III.B**, I have identified flaws with Dr. Rattray’s methodology.

---

<sup>7</sup> Graff Opening Report, Section IV.D.3.

<sup>8</sup> Rattray Report, ¶ 101.



**A. My Responses to Dr. Rattray's Issues with My Methodology**

14. Dr. Rattray misconstrues the scope of my assignment by faulting it for “not resembl[ing] any standard cybersecurity assessment.”<sup>9</sup> However, as I explained in my Opening Report, my assignment was to provide my analysis and opinions on a technical comparison between the state of SolarWinds’ cybersecurity depicted in (1) the Security Statement posted on its public website between 2017 and 2020 and (2) *internal assessments, presentations, and communications regarding the state of cybersecurity* during that same timeframe with respect to certain assertions in the Security Statement.<sup>10</sup> My assignment reflected the SEC’s allegation that “SolarWinds’ public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments about the Company’s cybersecurity policy violations, vulnerabilities, and cyberattacks.”<sup>11</sup> For this analysis, one does not need to attempt to conduct a retrospective cybersecurity assessment of SolarWinds years after the fact; rather, one needs to review how *SolarWinds employees assessed* the state of the company’s cybersecurity *at the time*, including their expressions of concern and warnings to each other about problems identified at SolarWinds.

15. Dr. Rattray also incorrectly argues that I cherry-picked “isolated” documents to review.<sup>12</sup> As discussed in the “Research Methodology and Analytical Framework” section of my

---

<sup>9</sup> Rattray Report, ¶ 101. (“[T]he process [Mr. Graff] follows does not resemble any standard cybersecurity assessment as such assessments are performed in the industry. [...] Cybersecurity assessments generally do not involve reviewing employees’ emails or presentations to management in the first place.”).

<sup>10</sup> Graff Opening Report, ¶ 17.

<sup>11</sup> Amended Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, February 16, 2024 (“Amended Complaint”), ¶ 1.

<sup>12</sup> Rattray Report, ¶¶ 101-102. (“Mr. Graff simply ignores all of that evidence, even though it is the core evidence that would inform a standard cybersecurity assessment. [...] [Mr. Graff’s] analysis consisted of zeroing in on isolated notations in emails, slide presentations, and other documents, and speculating about their meaning, while ignoring the context for them, including the sworn testimony of witnesses who wrote or knew about the notations at issue.”).

Opening Report, I identified relevant documents based on key word terms that relate to the Security Statement assertions I have been assigned to investigate, and compared the practices described in these internal documents to the widely accepted industry norms described in the Security Statement.<sup>13</sup> Dr. Rattray is also incorrect in stating that I ignored the context for these documents.<sup>14</sup> Just the opposite: as my Opening Report makes clear, I considered documentation and cited relevant witness testimony. Similarly, Dr. Rattray incorrectly opined that I “extrapolated” from “a limited number of” discrepancies with the Security Statement’s representations to conclude that these issues were “frequent.”<sup>15</sup> My Opening Report never stated anything about the frequency of an issue.<sup>16</sup> As I explained in my Opening Report, the types of major issues that slipped through SolarWinds’ internal controls need not materialize many times for them to indicate a systemic problem.<sup>17</sup>

---

<sup>13</sup> Graff Opening Report, ¶¶ 41-46.

<sup>14</sup> Rattray Report, ¶ 102. (“[Mr. Graff’s] analysis consisted of zeroing in on isolated notations in emails, slide presentations, and other documents, and speculating about their meaning, while ignoring the context for them, including the sworn testimony of witnesses who wrote or knew about the notations at issue.”).

<sup>15</sup> Rattray Report, ¶¶ 100, 106. (“Even if the issues [Mr. Graff] identified were major departures from SolarWinds’ stated practices [...] the magnitude of an issue has nothing to do with how frequent it is.”).

<sup>16</sup> Similarly, Dr. Rattray mischaracterized my analysis by trying to improperly inject into it a quantitative “benchmark for an expected or acceptable error rate.” (Rattray Report, ¶ 104.) My conclusion did not require the computation of an “error rate” because the benchmark to which I compared the practices described in SolarWinds’ internal documents was the industry norms to which the Security Statement asserted SolarWinds adhered. I was not trying to evaluate SolarWinds’ cybersecurity. I note that the concept of an “error rate” is unreasonable in the context of my assignment because it assumes that errors are equivalent in importance and can be assigned numerical values. However, not all vulnerabilities are of equal expected consequence. Indeed, the very goal of cybersecurity risk assessments is to ensure that companies focus their scarce resources on the most important areas (or, in this case, on the areas asserted to the public in the Security Statement). Attempts to capture qualitative information as a single numeric data point (such as an “error rate”) can miss the entire point of the exercise.

<sup>17</sup> For example, the fact that an intern was able to publicly expose an extremely weak password to a system that allows a hacker to upload malicious files that SolarWinds customers could subsequently download is, in and of itself, indicative of systemic problems related to both access control and user authentication. As remediation, an internal SolarWinds document from December 2020 stated that “There will be special training introduce[d] to ensure something like that does not happen anymore.” The fact that such training—and other, technical controls preventing such an issue—were not in place before reflects a systemic issue at SolarWinds. *See* SW-SEC00407702–707 at 702, 704; *and* Graff Opening Report, ¶¶ 77, 91.

16. Dr. Rattray also mischaracterized my opinion when he rebutted the argument—which I never made—that the representations in the Security Statement should be interpreted as “guarantees of perfection.”<sup>18</sup> The methodology that I employed in my Opening Report *never* assumed that SolarWinds had to attain a standard of perfection. On the contrary, as Dr. Rattray acknowledges, my Opening Report specifically stated that any organization diligently assessing its cybersecurity will uncover some routine issues needing to be addressed.<sup>19</sup> However, the cybersecurity problems reflected in the SolarWinds internal documents are not such routine issues; in fact, they are not the kind of problems that a company would encounter if it followed security best practices and industry norms in the manner described in the Security Statement.<sup>20</sup> Therefore, rather than comparing SolarWinds to a standard of perfection, my methodology compared SolarWinds to the cybersecurity norms and best practices that the company claimed to follow in its Security Statement.<sup>21</sup>

17. Dr. Rattray’s opinion that the cybersecurity issues I described in my Opening Report were “not events of significant magnitude” is not supported by evidence.<sup>22</sup> As I showed in my Opening Report, *SolarWinds’ own leadership and personnel* described these events as

---

<sup>18</sup> Rattray Report, ¶¶ 99, 103.

<sup>19</sup> Rattray Report, ¶ 103. *See* Graff Opening Report, ¶¶ 25, 50, 101, 136, 190.

<sup>20</sup> Graff Opening Report, ¶ 25.

<sup>21</sup> With respect to the cybersecurity norms and best practices that the Security Statement asserted that SolarWinds followed, Dr. Rattray incorrectly criticized me for purportedly “treat[ing] the Security Statement’s reference to NIST CSF as a standard requiring a company to meet some (undefined) set of ‘cybersecurity norms and best practices’” (Rattray Report, ¶ 113.). My Opening Report specifically stated that the NIST CSF is “not literally a standard,” and that I interpreted the Security Statement in the context of the cybersecurity norms because the Security Statement—explicitly and implicitly—refers to specific cybersecurity terminology, standard practices, and industry norms: “SolarWinds’ secure development lifecycle follows *standard security practices*,” and “*security best practices* are a mandated aspect of all development activities.” I therefore analyzed whether SolarWinds met those cybersecurity norms and best practices that the Security Statement asserted it did. *See* Graff Opening Report, ¶ 21 and SW-SEC00466120–142 (SolarWinds’ Security Statement) at 129, 132.

<sup>22</sup> Rattray Report, ¶ 107. (“[The examples Mr. Graff cites] are not events of significant magnitude. They are the sorts of issues that routinely come up at any cybersecurity program of significant size.”).

being of significant magnitude *at the time the incidents and vulnerabilities were uncovered*. For example, Chris Day (at the time of VP of Global DevOps and Technology Operations, currently SolarWinds' Chief Information Officer) characterized one of the security issues I describe in my Opening Report as "*a significant security and Sox [sic] violation*" that "*needs to stop immediately*."<sup>23</sup> Such contemporaneous internal SolarWinds declarations are in line with my opinion that these were significant security violations, based on my analysis comparing these SolarWinds practices to the security best practices and industry norms the company described in the Security Statement.<sup>24</sup> Dr. Rattray did not present evidence to support his opinion that these were "routine" issues.<sup>25</sup>

## **B. Dr. Rattray's Methodology Was Flawed**

### *1. The analysis that Dr. Rattray undertook did not "approximate the methodology" of a cybersecurity assessment*

18. Dr. Rattray stated that his methodology aimed to "approximate the methodology that [he] (and other cybersecurity experts) apply in conducting an external assessment of whether an organization has certain cybersecurity controls in place," where the "controls" that he undertook to "assess" were the "representations in the Security Statement that are challenged in the SEC's Amended Complaint."<sup>26</sup> Based on my experience,<sup>27</sup> the analysis that Dr. Rattray undertook was not a cybersecurity assessment, as I explain below.

---

<sup>23</sup> SW-SEC00254254–266 at 265.

<sup>24</sup> Graff Opening Report, ¶ 25.

<sup>25</sup> Rattray Report, ¶ 107. ("They are the sorts of issues that routinely come up at any cybersecurity program of significant size.").

<sup>26</sup> Rattray Report, ¶¶ 17, 21.

<sup>27</sup> I have personally performed formal cybersecurity assessments at national security installations such as the Los Alamos National Laboratory and Lawrence Livermore National Laboratory, and have assisted businesses in their

19. First, Dr. Rattray did a partial survey of policies and looked at some of the processes SolarWinds had during the Relevant Period. But he did *not* assess whether those policies and processes were enforced, or the extent to which the implementation of the policies was consistent with the Security Statement. For example, the SARF forms are evidence relevant to SolarWinds’ access control policies but are not themselves definitive evidence of whether those policies were in fact enforced or implemented. To assess a program, one needs to not only review the forms that were filled out, but also check the forms against records of what actually occurred, *e.g.*, account creation on a given date.<sup>28</sup> Instead, Dr. Rattray appeared to rely heavily on deposition testimony without independently assessing whether the testimony was correct.

20. Dr. Rattray repeatedly acknowledges the existence of evidence showing that SolarWinds did not conform to the security practices asserted in its Security Statement.<sup>29</sup> However, he dismisses (without evidence) such pieces of information as “the sorts of issues that routinely come up at any cybersecurity program of significant size,”<sup>30</sup> and concludes that—even if they were not precisely followed—“processes and procedures were in place.”<sup>31</sup> Dr. Rattray’s

---

own such assessments. Additionally, as CISO of NASDAQ OMX, I oversaw external cybersecurity assessments conducted by teams from the Department of Homeland Security, Microsoft, and Mandiant. That work was consistent with what I did at the National Laboratories, and it was consistent with what NIST recommends.

<sup>28</sup> Whether or not SolarWinds itself did perform an audit, as with the User Access Reviews (UARs), Dr. Rattray himself certainly did not.

<sup>29</sup> *See, e.g.*, Rattray Report, ¶ 190 (“[A]ll that was happening here was that developers were working *inside* the production environment.”); ¶ 128 (“[C]ustomer support representatives did not always need full admin access in performing that role, and there were risks associated with that level of access—as highlighted by a recent incident where data in a customer environment had been accidentally altered by SolarWinds personnel.”).

<sup>30</sup> *See, e.g.*, Rattray Report, ¶ 107.

<sup>31</sup> Rattray Report, ¶ 120. (“Even if some forms might not be filled out entirely correctly or if errors were sometimes made in the process, the fact remains that processes and procedures were in place.”); ¶ 126 (“This incident does not evidence any systemic lack of role-based access controls at SolarWinds. If anything, it further evidences that role-based access controls were in place.”); Footnote 158 (“The fact that SolarWinds occasionally identified, over a multi-year period, a small number of employees or contractors— out [of] thousands who worked for the company— whose access may not have been promptly revoked upon termination does not imply that it lacked processes and procedures for deprovisioning access of terminated personnel.”).

assertion that “processes and procedures were in place” entirely misses the point. From a security perspective, the question was never which policies SolarWinds had; the question is whether such policies and practices are consistently implemented in accordance with the Security Statement.

2. *Dr. Rattray relied upon non-existent qualifying language in the Security Statement*

21. In his analysis, Dr. Rattray improperly relied upon qualifying language that does not, in fact, exist in the Security Statement.<sup>32</sup> For example, the Security Statement asserts that “SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect, and respond to security incidents.”<sup>33</sup> However, Dr. Rattray “underst[ood] the representation about the NIST CSF in the Security Statement in the same way” as the following statements from General Motors, Digital Realty Trust, and SkyWest:<sup>34</sup>

**General Motors:** “We design and assess our program based on the [...] (NIST CSF). **This does not imply that we meet any particular technical standards, specifications, or requirements, but rather that we use the NIST CSF as a guide to help us identify, assess, and manage** cybersecurity risks relevant to our business [emphasis added].”<sup>35</sup>

**Digital Realty Trust:** “We utilize the [...] (NIST CSF) in considering the design and in assessing our processes. **This does not imply that we meet any particular technical standards, specifications, or requirements, only that we use the NIST CSF**

<sup>32</sup> As I pointed out in my Opening Report, the Security Statement contained little qualifying language indicating that assertions of the Security Statement might not be consistently followed. For example, while the Security Statement noted that “SolarWinds *strives* to apply the latest security patches and updates,” it did not use similar language (such as “strives”) with respect to the other assertions. In fact, many sentences explicitly used language indicating categorical assertions. *See* Graff Opening Report, ¶ 47. *See also*, SW-SEC00466120–142 (SolarWinds’ Security Statement) at 129–132.

<sup>33</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

<sup>34</sup> Rattray Report, ¶ 112.

<sup>35</sup> General Motors Financial Company, Inc., SEC Form 10-K, filed December 31, 2023.

**as a guide to help us identify, assess, and manage** cybersecurity risks relevant to our business [emphasis added].”<sup>36</sup>

**SkyWest:** “[W]e have aligned our processes with the [...] (NIST CSF) and assess our cybersecurity maturity against the NIST CSF’s core functions; **however, this does not imply that we meet any particular technical standards, specifications or requirements, only that we use the NIST CSF as a guide to help us identify, assess and manage** cybersecurity risks relevant to our business [emphasis added].”<sup>37</sup>

22. Dr. Rattray provided no explanation or evidence as to why he understood the Security Statement’s representation about the NIST CSF as a statement that SolarWinds “used the NIST CSF as a guide” in assessing its cybersecurity posture.<sup>38</sup> In fact, the examples of the language by General Motors, Digital Realty Trust, and SkyWest—which do state that they used the NIST CSF as a guide only and added the caveat that this “does not imply that we meet any particular technical standards, specifications, or requirements”—underscore that this type of qualifying language was *missing* from SolarWinds’ Security Statement.<sup>39</sup>

23. Dr. Rattray also added non-existent qualifying language in the Security Statement’s discussion of passwords,<sup>40</sup> interpreting SolarWinds’ assertion as “SolarWinds automatically requir[ing] the use of complex passwords *where it was feasible to do so, i.e., where the system could be configured to enforce password complexity.*”<sup>41</sup> Dr. Rattray’s

<sup>36</sup> Digital Realty Trust, Inc., SEC Form 10-K, filed December 31, 2023.

<sup>37</sup> Skywest, Inc., SEC Form 10-K, filed December 31, 2023.

<sup>38</sup> Rattray Report, ¶ 112.

<sup>39</sup> Additionally, unlike SolarWinds, these companies also did not claim to “follow” the NIST CSF; instead, they used the correct and clear language that they “design” and “assess” their cybersecurity program based on the NIST CSF.

<sup>40</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. (“Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.”).

<sup>41</sup> Rattray Report, ¶ 175. [emphasis added] (“[T]he most sensible way to read this statement is that SolarWinds automatically required the use of complex passwords where it was feasible to do so.”).



interpretation of the Security Statement is incorrect: the qualifying language that Dr. Rattray relied upon was *missing* from the Security Statement. In fact, SolarWinds’ Security Statement says the opposite—that its password policy “covers *all* applicable information systems, applications, and databases [emphasis added].”<sup>42</sup>

#### IV. ACCESS CONTROLS

24. As I explain in this section, Dr. Rattray’s statements that my conclusions regarding SolarWinds’ access controls were “[e]xtrapolat[ed] from isolated events”<sup>43</sup> are both speculative and unsupported by the evidence. My conclusion from my Opening Report remains unchanged: these incidents are indicative of systemic problems which show that SolarWinds did not consistently follow the assertions in the Security Statement regarding access controls.

##### A. Dr. Rattray’s Analysis of SolarWinds Developers’ Access to Production Data Is Flawed

25. Dr. Rattray’s response to the fact that SolarWinds developers had high-privilege (“SuperUser”) access through a shared account to billing data from the production environment is deeply flawed and contradicted by internal SolarWinds documents.<sup>44</sup>

26. First, Dr. Rattray’s opinion that this incident was not of significant magnitude<sup>45</sup> is directly contradicted by an internal email from Chris Day (SolarWinds’ current CIO), who considered this incident to be “a significant security [...] violation” that “needs to stop

---

<sup>42</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

<sup>43</sup> Rattray Report, Section IV.C.1.

<sup>44</sup> Rattray Report, ¶ 121. I discussed this incident extensively in my Opening Report, Sections IV.B-D.

<sup>45</sup> Rattray Report, ¶ 124. (“First of all, this was not a ‘problem’ of significant ‘magnitude.’”).



immediately.”<sup>46</sup> Based on my experience, I concur with Mr. Day about the significance of the problem, as well as the urgent need to separate development and production environments.<sup>47</sup>

27. Second, in my opinion, Dr. Rattray’s suggestion that the only risk SolarWinds faced was “the risk that [developers] might accidentally modify the data, or the highly remote risk that they would intentionally modify it,”<sup>48</sup> is incorrect. In addition to the possibility that developers could potentially modify the underlying usage to change the amounts that customers were charged, or pass a customer’s information on to its competitors, the sharing of high privilege accounts may also make it more difficult to prevent, detect, and remediate malicious behavior.<sup>49</sup> In his report, Dr. Rattray also failed to fully consider the risk from outside threats, since expert attackers often make it a special point to gain unauthorized access to highly privileged accounts as a means of compromising system security protections including access controls.<sup>50</sup>

28. Third, Dr. Rattray’s portrayal of this incident as a “one-off issue”<sup>51</sup> was also contradicted by internal SolarWinds documents. As I wrote in my Opening Report, a SolarWinds

---

<sup>46</sup> SW-SEC00254254–266 at 265.

<sup>47</sup> SW-SEC00254254–266 at 265. (“Under no circumstances is development to be done in production.”).

<sup>48</sup> Rattray Report, ¶ 124. (“While SuperUser access came with ‘write’ access, the only risks from granting that access were the risk that they might accidentally modify the data, or the highly remote risk that they would intentionally modify it. And this was merely *billing* data; it was sensitive from a SOX perspective, because it related to SolarWinds’ financial reporting, but it had nothing to do with the security of SolarWinds’ products.”).

<sup>49</sup> Graff Opening Report, ¶¶ 81, 83.

<sup>50</sup> Graff Opening Report, ¶ 81. For example, if expert attackers got access to SolarWinds’ billing data, they might have been able to easily identify the list of customers of each SolarWinds product. And, attackers able to compromise a specific SolarWinds product, may also be able to identify which customers could be vulnerable due to their use of this product.

<sup>51</sup> Rattray Report, ¶ 121. (“Developer Access to Billing Data for Test Purposes. Mr. Graff’s other hasty generalizations [...] concern one-off issues with marginal if any relevance to SolarWinds’ procedures for provisioning users with access rights.”).

Senior Product Manager characterized this issue as “not something new,” and stated that SolarWinds “develop[ed] billing using production services *since the beginning*.”<sup>52</sup>

29. Fourth, Dr. Rattray’s conclusion that this incident “evidences that role-based access controls were in place” because the developers “did not themselves have the access they sought” is irrelevant.<sup>53</sup> While developers did not seem to have been provisioned with “SuperUser” access to the production billing data in an official capacity, the main issue is that the developers should never have had access to the production environment in the first place.<sup>54</sup> And, yet, they accessed the data through a shared account, which violated industry best practices, as well as multiple statements in the Security Statement,<sup>55</sup> regardless of whether it was eventually detected and remediated.

30. Fifth, Dr. Rattray ignored<sup>56</sup> that solutions SolarWinds proposed to this issue would retain the problematic connection between the development and production environments, and would thus continue to violate industry best practices and the assertions in the Security

---

<sup>52</sup> Graff Opening Report, ¶ 156; SW-SEC00254254–266 at 264–265. (From Andrey Rodushkin, Senior Product Manager: “As far as I know it’s not something new, we were developing billing using production services since the beginning as only production has data to test billing.”). [Emphasis added.]

<sup>53</sup> Rattray Report, ¶ 126. (“If anything, [this incident] further evidences that role-based access controls were in place. The developers at issue did not themselves have the access they sought. They at first improperly borrowed an account of another employee to obtain it; but that was detected as a security violation.”).

<sup>54</sup> Graff Opening Report, ¶ 84.

<sup>55</sup> First, providing unnecessary access to highly privileged accounts is inconsistent with the Security Statement assertion that “[r]ole based access controls are implemented for access to information systems.” Second, using shared logins is inconsistent with the Security Statement assertion that “[w]e require that authorized users be provisioned with unique account IDs.” Third, developers accessing the production dataset is inconsistent with the Security Statement assertion that “SolarWinds maintains separate development and production environments.” SW-SEC00466120–142 (SolarWinds’ Security Statement) at 131–132.

<sup>56</sup> Rattray Report, ¶ 123. (“The solution arrived at was to (a) give the developers SuperUser accounts for the time being so that they could continue working on the project and (b) eventually create a special ‘read-only’ level of access that the developers could use, once the relevant engineering resources freed up to do that work.”).

Statement.<sup>57</sup> Ultimately, Dr. Rattray failed to recognize that the poor implementation in this incident increased the company’s cybersecurity risks and violated at least three assertions in the Security Statement (and related industry best practices) about Access Control, User Authentication, and Secure Software Development.<sup>58</sup>

**B. Dr. Rattray’s Analysis of SolarWinds’ Exposure of the Password “solarwinds123” Is Flawed**

31. Dr. Rattray also incorrectly suggested that an incident in which an extremely weak password (“solarwinds123”) to a sensitive system was accidentally made publicly available<sup>59</sup> did not indicate problems with SolarWinds’ access controls.<sup>60</sup>

32. However, despite Dr. Rattray’s suggestion to the contrary,<sup>61</sup> the fact that this password leak was an accident (and not an intentional action on SolarWinds’ part) is irrelevant to the question of whether SolarWinds’ practices were consistent with the Security Statement. That

---

<sup>57</sup> Even assuming for argument’s sake that granting the developers of this billing project read-only access to the database was reasonable and necessary, the short-term solution included write-level permissions for individuals whose job functions did not require them. While the long-term solution revoked “write” access to the billing data, it nonetheless still allowed developers to access production data, failing to separate development from production environment. SW-SEC00254254–266 at 255.

<sup>58</sup> See footnote 55.

<sup>59</sup> This extremely weak password was to an FTP account that allowed users to “upload anything to downloads.solarwinds.com,” which was made publicly available at a code repository. SW-SEC00407702–707 at 702, 704. See also, SW-SEC00001476–484 at 484 (“We have received an inquiry about hard-coded credentials, which are publicly available and allows attacker to upload files to our FTP download server”); SW-SEC00001464 (an email sent by PSIRT to InfoSec team on November 19, 2019) (“Hi Team, I have found a public Github repo which is leaking ftp credential belongs to SolarWinds. [...] Username: solarwindsnet Password: solarwinds123 [...] Via this any hacker could upload malicious exe and update it with release SolarWinds product.”); SW-SEC00001476–484 at 483 (“This was a previous password for the main Akamai Upload Account. It was still in an active state.”).

<sup>60</sup> Rattray Report, ¶ 133. (“Mr. Graff appears to infer from this incident that SolarWinds lacked role-based access controls.”).

<sup>61</sup> Rattray Report, ¶ 133. (“Obviously, SolarWinds did not intentionally grant ‘the public’ access to the FTP account in question. Due to an *accident*, there was a *risk* that an unauthorized person could gain access to the account [emphasis in original]. But that does not imply that SolarWinds had a policy of freely allowing anyone to access the account or that it generally lacked processes and procedures for limiting user access based on their role.”).

even an intern working on “his bachelor thesis” was able to publicly expose an extremely weak password to a system that, according to Mr. Brown,<sup>62</sup> allows hackers to distribute malware directly to SolarWinds customers by disguising malware as a legitimate SolarWinds product is, in and of itself, indicative of a systemic issue.<sup>63</sup> The fact that an incident of this magnitude could develop indicates poor access control practices that were contrary to those described in the Security Statement.

**C. Dr. Rattray Incorrectly Argued that I Drew “Inferences from Isolated Notations in Documents”**

33. Below I provide examples of why Dr. Rattray’s argument that I drew conclusions from “isolated” notations is incorrect.<sup>64</sup>

34. First, Dr. Rattray suggested that a document that reads “[c]oncept of least privilege not followed as a best practice”<sup>65</sup> does not mean that least privilege was not followed as a best practice.<sup>66</sup> Despite his assertion that I ignored relevant testimony from Eric Quitugua,<sup>67</sup>

---

<sup>62</sup> SW-SEC00407702–707 at 702. (“[Mr. Brown:] With that credential they could upload anything to downloads.solarwinds.com [...] In their POC [proof of concept] they uploaded a file to the site. I have made an assumption that this is our main download site since [we] needed to confirm the download site with on internal checksums [sic]. The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site.”).

<sup>63</sup> I discussed this topic in my Opening Report. *See, for example*, Graff Opening Report, ¶ 91.

<sup>64</sup> Rattray Report, ¶ 116. (“First, [Mr. Graff] takes isolated events or issues and makes hasty generalizations from them, in order to conclude that SolarWinds broadly failed to implement role-based access controls or the principle of least privilege, when that is simply not what the cited documents show. Second, he takes vague remarks in various documents out of context and treats them as admissions of systemic failures, when that interpretation is not supported by the evidence and is specifically contradicted by the people who actually wrote the remarks.”).

<sup>65</sup> SW-SEC00012265–275 at 268.

<sup>66</sup> Rattray Report, ¶ 137. (“Nowhere, however, does this document indicate that this notation was meant as any sort of finding that SolarWinds generally did not set access controls on a least-privilege necessary basis. The notation appears under the heading ‘Issues, Risks, & Dependencies.’ It is not clear that it was meant to be a finding at all, as opposed to being a statement of the concern that the project the slide described—an audit of user privileges—was meant to address. In other words, the notation could simply have meant that the purpose of the project was to check whether the concept of least privilege was not being followed as a best practice.”).

<sup>67</sup> Rattray Report, ¶ 138.

my Opening Report considered the testimony of SolarWinds employees regarding this issue, including Mr. Quitugua.<sup>68</sup> According to Mr. Quitugua's testimony, SolarWinds identified that, "for whatever reason," a subset of systems "weren't following the best practices that we described [in the Security Statement regarding the concept of least privilege]."<sup>69</sup> Additionally, as I described in my Opening Report, I also saw several internal documents supporting Mr. Quitugua's testimony that "not all systems [...] were following best practice" regarding the least privilege principle.<sup>70</sup> I did not find anything in Mr. Quitugua's testimony that would change my conclusion that SolarWinds failed to follow the least privilege principle in line with the Security Statement.

35. Second, Dr. Rattray's opinion about an October 2018 help-desk ticket was sheer speculation.<sup>71</sup> He had various theories as to why SolarWinds employees granted access rights to a temporary worker for an ad-hoc one year period without a known termination date.<sup>72</sup> However, despite reportedly having reviewed "samples from thousands of these tickets,"<sup>73</sup> Dr. Rattray did

---

<sup>68</sup> Graff Opening Report, Section IV.B.3.a.

<sup>69</sup> Investigative Testimony of Eric Quitugua - Vol. II, September 1, 2021 ("Quitugua Investigative Testimony, Vol. II"), September 1, 2021 ("Quitugua Investigative Testimony, Vol. II"), at 280:13-281:4. ("Q. In this early 2018 timeframe, was the concept of least privilege not being followed throughout the SolarWinds organization? A. We identified, you know, as part of our internal audits and checks that not all systems which were under IT control were following best practice. Q. Okay. And I think we had looked again previously at the detailed security statement, and the detailed security statement indicated that SolarWinds did follow the concept of least privileged, correct? A. Yes. Q. So what you're telling me is that at least with respect to some systems, that wasn't the case? A. For a subset of systems that we identified, they weren't -- you know, for whatever reason, we identified that they weren't following the best practices that we described.").

<sup>70</sup> Graff Opening Report, Section IV.B.3.a.

<sup>71</sup> Rattray Report, ¶¶ 118-119, discussing SW-SEC-SDNY\_00050922 at 922.

<sup>72</sup> Rattray Report, ¶ 119. ("[I]t is not even clear from the [ticket] chat that the '1 year' [termination] period was incorrect; the person who specified the time period may have gotten it from the temp's manager, or that period may have been a standard employment period for a temp. [...] To the extent Mr. Graff makes that assumption, he ignores the testimony and evidence reflecting that a separate SARF would be submitted upon an employee's termination, which would have caused the temp's access to have been deprovisioned regardless of any end date listed on their original SARF.").

<sup>73</sup> Rattray Report, ¶ 45.

not provide any evidence to support his argument. Therefore, Dr. Rattray’s speculative conclusions do not show that SolarWinds’ access rights policies were being followed in line with the Security Statement’s assertion. The ad-hoc processes that SolarWinds employees followed are not consistent with the assertions in the Security Statement.

36. Third, Dr. Rattray also improperly dismissed an issue pertaining to certain SolarWinds support staff having what an internal November 2019 document described as “excessive” and “inappropriate” system-level access to MSP customer systems.<sup>74</sup> “Excessive” and “inappropriate” access clearly violates the least privilege principle (and thus the Security Statement),<sup>75</sup> whether or not it was, as Dr. Rattray argued, “limited to a discrete set of employees.”<sup>76</sup> In fact, the November 2019 presentation suggested that an “Anticipated Outcome” of the proposed engineering project to implement security improvements was to have “[s]upport roles aligned with least privilege.”<sup>77</sup> Thus, this presentation is consistent with SolarWinds employees being aware that the support roles were not aligned with the least privilege principle.<sup>78</sup>

---

<sup>74</sup> SW-SEC00631418–427 (Presentation, “MSP Support Security Improvement,” November 2019), at 419. (“MSP Support staff has a significant level of system level access to both MSPs and MSP customers. The level of access is excessive and if abused poses a significant insider threat. [...] Recent incidents have involved support staff and engineering’s inappropriate access to customers environments.”).

<sup>75</sup> As I explained in my Opening Report, allowing an “excessive” level of access to customer assets directly contradicted the assertion in the SolarWinds Security Statement that access was set on a “need-to-know / least privileged necessary” basis. With “system level access to both MSPs and MSP customers,” SolarWinds’ employees could take complete control over a customer’s system. Provisioning employees with unnecessary system-level access is a serious access control issue that can allow users to take complete control over a computer. Users would be able to read, overwrite, and delete anything on a system; crash the system; remove other users’ accounts; or grant system-level access to other users. Graff Opening Report, ¶¶ 70-71.

<sup>76</sup> Rattray Report, ¶ 129. (“This was an edge case in which access to MSP customer systems was already limited to a discrete set of employees who needed access to those systems in order to perform their role. SolarWinds was simply considering how to limit their access even further in response to a particular risk being identified.”).

<sup>77</sup> SW-SEC00631418–427 (Presentation, “MSP Support Security Improvement,” November 2019), at 419.

<sup>78</sup> Graff Opening Report, ¶ 72.

37. In my experience, characterizing the above instances as “isolated” is incorrect; in fact, they show systemic issues. For example, as Dr. Rattray acknowledges, creating a read-only (i.e., not “excessive”) customer support account “would have required engineering work on SolarWinds’ MSP customer support system.”<sup>79</sup> Similarly, with respect to developers’ inappropriate access to production data, Dr. Rattray acknowledged that “[t]here was not an existing ‘read-only’ level of privilege that could be provided for the systems in question; and creating one would require engineering work that would take time.”<sup>80</sup> The fact that it takes time-consuming engineering work to bring SolarWinds’ system in line with the least privilege principle shows that SolarWinds’ system was structurally unprepared to adhere to the least privilege principle it claimed to follow in the Security Statement. In other words, these incidents are not “routine” issues where SolarWinds staff incidentally used “write” accounts when “read” accounts were also available; “read” accounts did not even exist. This is like claiming that a car adheres to standard security features when in fact it does not have seatbelts: the issue is not that the passengers chose not to fasten seatbelts; it’s that the seatbelts did not even exist for them to fasten.

**D. Dr. Rattray’s Dismissal of SolarWinds’ FedRAMP Assessment Is Unsupported**

38. Dr. Rattray disputed my reliance on the 2019 FedRAMP Assessment, but his reasons for doing so were incorrect.

---

<sup>79</sup> Rattray Report, ¶ 128. (“So this deck appears to have been proposing various technical changes to limit the scope of the access that support staff had, including the creation of a new read-only type of customer support account separate from an admin account, which would have required engineering work on SolarWinds’ MSP customer support system in order to implement.”).

<sup>80</sup> Rattray Report, ¶ 123.



39. First, Dr. Rattray dismissed the FedRAMP assessment as a “budgeting exercise—not a security exercise.”<sup>81</sup> However, the purpose of the study is not particularly relevant to my assignment. The *issues* that it delineated about the state of SolarWinds’ cybersecurity controls, on the other hand, are relevant to the question of the Security Statement’s accuracy, which was within the scope of my analysis.

40. Second, Dr. Rattray dismissed the FedRAMP assessment because “FedRAMP is a highly demanding set of federal standards.”<sup>82</sup> However, this—again—is irrelevant to my analysis, because, in my Opening Report, I did not hold SolarWinds to the federal standards required by FedRAMP. Rather, I relied on this document for its informative value regarding specific SolarWinds cybersecurity controls to which the Security Statement asserted SolarWinds adhered.

41. Third, Dr. Rattray argued that Ms. Pierce did not have the technical expertise to conduct an assessment of SolarWinds’ implementation of security controls.<sup>83</sup> However, as Dr. Rattray described and Ms. Pierce testified, her role in the company was to “gather[] documentation and information from other people and track[] tasks,”<sup>84</sup> as reflected by her

---

<sup>81</sup> Rattray Report, ¶ 142. (“SolarWinds’ cloud business line wanted to be able to sell its products to the federal government, but Ms. Johnson believed that complying with FedRAMP would be ‘very expensive’ because the standards were difficult to meet and would require extensive formal documentation approved by an outside third-party assessor. It was in this context that Ms. Johnson asked Ms. Pierce to do a ‘very cursory, very preliminary’ assessment of how much cost and effort would be involved in trying to obtain FedRAMP certification, as it was believed that the expected investment would not be worth the expected return from increased sales. In other words, the assessment was a *budgeting* exercise—not a security exercise.”).

<sup>82</sup> Rattray Report, ¶ 142.

<sup>83</sup> Rattray Report, ¶ 148.

<sup>84</sup> Rattray Report, ¶ 141; Deposition of Kellie Jaie Pierce, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, July 24, 2024 (“Deposition of Kellie Jaie Pierce”), at 28:19-29:7. (“[M]ost of these [evaluations] I could coordinate. I could find the NIST framework, put it in a document and often work with others to -- for input and then make [...] my best guess, not as a technical person and not as an auditor, to evaluate, you know, where I felt the -- if we were meeting or, like, able to achieve that particular control. Q. All right. And so how -- if you didn’t have the sort of technical background, how were you able to make that best guess



comments in the FedRAMP assessment.<sup>85</sup> Being in this coordination role, and working—as Dr. Rattray described—“under Rani Johnson and Tim Brown,” would have put Ms. Pierce in a good position to ascertain whether SolarWinds had various policies in place, by checking with the appropriate technical personnel and managers who had the requisite knowledge.<sup>86</sup>

## V. PASSWORDS AND USER AUTHENTICATION

42. Dr. Rattray incorrectly concluded that the password and user authentication related problems presented in my Opening Report “at most, suggest that SolarWinds occasionally identified gaps in its policies that were remediated.”<sup>87</sup> As explained in my Opening Report, the discrepancies between SolarWinds’ internal documents and Security Statement within this area reflect significant deviations from industry norms, with potential company-wide impact.<sup>88</sup>

---

whether you were meeting the criteria or not? A. Often I would have a third-party auditor. We would have external people look at things. Or I would solicit information from product managers or leadership.”).

<sup>85</sup> The FedRAMP Assessment reflects that Ms. Pierce consulted with SolarWinds’ product managers in preparing this assessment. *See, e.g.*, SW-SEC00045358 at tab “MODERATE SUMMARY KP,” cell G24-G28 (“Agree with PM [product manager]”). *See also*, Deposition of Kellie Jaie Pierce, at 48:21-49:7. (“I downloaded this on the Excel document, the FedRAMP [...] controls and circulated that with the product managers for [...] this assessment. [...] [T]he product managers have the technical -- more technical expertise than I would on if their product would meet this -- meet the control or -- and so circulated with them and then compiled the information and just scored it with a red, yellow or green.”).

<sup>86</sup> Additionally, she was commissioned by the security leadership to undertake the FedRAMP survey. If SolarWinds’ leadership did not believe she was qualified to undertake the analysis with which she was tasked, that would itself raise troubling red flags about SolarWinds’ adherence to cybersecurity best practices.

Dr. Rattray also asserted that I mischaracterized the role of Ms. Pierce at the company: “Ms. Pierce was not the ‘Director of Security’ at SolarWinds. She was a ‘program manager’ who worked under Rani Johnson and Tim Brown.” (Rattray Report, ¶ 141.) However, Ms. Pierce herself testified that she was the “Security, privacy and compliance director from February 2019 to June 2021.” (Deposition of Kellie Jaie Pierce, at 17:17-18:1.)

<sup>87</sup> Rattray Report, ¶ 158. (“Instead, as with access controls, he focuses on a small number of events and notations in documents that, at most, suggest that SolarWinds occasionally identified gaps in its policies that were remediated. It is commonplace and expected—even for companies with the most stringent security regimes—to identify these sorts of issues from time to time.”).

<sup>88</sup> Graff Opening Report, ¶ 136.

43. First, Dr. Rattray’s criticism that instances of employees using shared accounts were “flagged as a security violation”<sup>89</sup> and “detected and remediated”<sup>90</sup> does not negate the fact that these *were* violations of the Security Statement’s assertion that SolarWinds “require[s] that authorized users be provisioned with unique account IDs.”<sup>91</sup> Dr. Rattray also confused prevention with ex-post remediation: SolarWinds’ ad-hoc and retroactive attempts to remediate cases where accounts were shared do not show, as Dr. Rattray argued, that SolarWinds took steps to “prevent” this issue.<sup>92</sup> Additionally, Dr. Rattray’s argument that SolarWinds had a policy about not using shared accounts is irrelevant to assessing whether SolarWinds’ practices were consistent with the Security Statement.<sup>93</sup> Regardless of what SolarWinds’ policies said, accounts *were* being shared in a way contrary to the Security Statement,<sup>94</sup> which was a problem recognized by senior SolarWinds employees at the time.<sup>95</sup>

44. Similarly, Dr. Rattray’s characterization of my conclusion related to hard-coding passwords is inaccurate. Despite Dr. Rattray’s suggestion, I never stated that hard-coding

---

<sup>89</sup> Rattray Report, ¶ 166. (“But as the email itself indicates, this was flagged as a security violation, which is why the developers were requesting that ‘SuperUser’ access be added to their own accounts.”).

<sup>90</sup> Rattray Report, ¶ 167. (“[Mr. Graff] treats instances in which the company detected and remediated violations of a policy as evidence that the company *lacked* a policy.”).

<sup>91</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement).

<sup>92</sup> Rattray Report, ¶ 161. (“None of the documents Mr. Graff cites suggests that SolarWinds had any general policy or practice of allowing accounts to be shared. To the contrary, they show that SolarWinds did not allow sharing of accounts and took steps to prevent it.”).

<sup>93</sup> Rattray Report ¶ 161 (“The mere fact that sharing of certain accounts was occasionally detected at SolarWinds does not imply that SolarWinds lacked a general practice of provisioning users with unique account IDs.”); ¶ 167 (“Part of *having* a policy is using it as a standard to detect and remediate nonconformance.”).

<sup>94</sup> Graff Opening Report, Section IV.C.3.a.

<sup>95</sup> *See, e.g.*, Rattray Report, ¶ 162 (“Mr. Quitugua had discovered instances where service accounts intended for use by an application were being used by individual members of the relevant application team in the course of their work, which was not best practice.”) and ¶ 166 (“[T]he developers had previously been using credentials borrowed from a different SolarWinds employee who had ‘SuperUser’ access.”).

passwords in configuration files was “allowed.”<sup>96</sup> Instead, the issue that I identified is that passwords *were* hard-coded in a way contrary to the “password best practices” described in the Security Statement.<sup>97, 98</sup>

45. Additionally, despite Dr. Rattray’s assertion to the contrary,<sup>99</sup> it was Mr. Brown (and not me) who stated that SolarWinds’s inappropriate exposure of a password effectively made it possible for hackers to distribute malware directly to SolarWinds customers by disguising malware as a legitimate SolarWinds product. As Mr. Brown wrote to his colleagues in a December 2020 email when discussing an incident exposing a hard-coded password: “With that credential they could upload anything to downloads.solarwinds.com [....] The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site.”<sup>100</sup>

46. Dr. Rattray’s suggestion that this was not a serious incident because there were “compensating controls” in place<sup>101</sup> is belied by both contemporaneous documents and Mr. Brown’s own characterization of the impact of this incident. First, in his December 2020

---

<sup>96</sup> Rattray Report, ¶ 170. (“Mr. Graff cites only two instances where this [hard-coding passwords in configuration files] was identified, and in both instances the hard-coding was not allowed but instead was flagged for remediation.”).

<sup>97</sup> Graff Opening Report, Section IV.C.3.b.i.

<sup>98</sup> Dr. Rattray is incorrect in arguing that “the only ‘best practices’ the Security Statement mentions relate to automatically enforcing password complexity.” Rattray Report, ¶ 169. The Security Statement discusses “password best practices” in general—among which is “the use of complex passwords.” *See* SW-SEC00466120–142 (SolarWinds’ Security Statement).

<sup>99</sup> Rattray Report, ¶ 173. (“Mr. Graff overstates the magnitude of the incident. He states that the exposure of the password made it possible for hackers to distribute malware to SolarWinds customers.”).

<sup>100</sup> SW-SEC00407702–707 at 702. Graff Opening Report, ¶ 91.

<sup>101</sup> Rattray Report, ¶ 173. (“Mr. Graff overstates the magnitude of the incident. He states that the exposure of the password made it possible for hackers to distribute malware to SolarWinds customers, but he ignores compensating controls that were in place. As noted earlier, software issued by SolarWinds would bear the company’s digital signature, a form of validation that companies commonly check for before installing software updates; so any malware uploaded to the site by someone else would likely have been quickly detected.”).

email, Mr. Brown cautioned his colleagues stating: “This was managed and resolved quickly but *it did take place* [emphasis added] and a very weak password existed to access that environment [that could have corrupted one of our downloads].”<sup>102</sup> Second, more than a year after this incident was discovered, an internal SolarWinds document stated that “There will be special training introduce[d] to ensure something like that does not happen anymore.”<sup>103</sup> The fact that such training—and other, technical controls preventing such an issue—were not already in place reflects a systemic issue at SolarWinds. Third, Dr. Rattray’s argument that “any malware uploaded to the site by someone else *would likely have been* quickly detected [emphasis added]”<sup>104</sup> is speculative and does not take into account the fact that technical methods exist to defeat many common digital signature validation methods.<sup>105</sup>

47. Finally, Dr. Rattray’s statements related to password complexity are also irrelevant and incorrect. His argument that it was only “a *single* instance [...] out of many thousands of accounts” that SolarWinds employees used the extremely weak password of “solarwinds123” is irrelevant when evaluating whether SolarWinds’ practices were in line with the password best practices it asserted in the Security Statement.<sup>106</sup> The fact that SolarWinds’ internal controls were not able to catch an undergraduate intern setting such a weak password to

---

<sup>102</sup> SW-SEC00407702–707 at 702.

<sup>103</sup> SW-SEC00407702–707 at 704.

<sup>104</sup> Rattray Report, ¶ 173.

<sup>105</sup> See, e.g., MITRE, “CAPEC-459: Creating a Rogue Certification Authority Certificate,” July 31, 2018, <https://capec.mitre.org/data/definitions/459.html>; Zetter, Kim, “Hackers Breached Adobe Server in Order to Sign Their Malware,” Wired, September 27, 2012, <https://www.wired.com/2012/09/adobe-digital-cert-hacked/>.

<sup>106</sup> Rattray Report, ¶ 176. (“Second, in any event this was, again, a *single* instance of an account having a noncomplex password—out of many thousands of accounts that SolarWinds would have maintained during the Relevant Period. Mr. Graff provides no basis to infer from this incident that the use of non-complex passwords was any sort of pervasive problem at SolarWinds.”).

a sensitive system<sup>107</sup> is, in and of itself, indicative of a systemic issue (indeed, it was an outsider who pointed out this issue to SolarWinds).<sup>108</sup> Even if the incident materialized only once, the fact that an incident of this magnitude could develop indicates a systemic failure of internal controls. The fact that both Mr. Brown and Mr. Quitugua acknowledged that using such a weak password was likely not a one-time occurrence<sup>109</sup> precisely proves my argument that this was a systemic failure of controls. Simply put, SolarWinds did not have a system in place to ensure that the assertion in the Security Statement about password complexity was correct.<sup>110</sup>

48. I note that Dr. Rattray’s description of SolarWinds’ practices regarding bug bounty programs and the remediation of the “solarwinds123” incident is again irrelevant when evaluating whether SolarWinds’ practices were in line with the password best practices it asserted in the Security Statement.<sup>111</sup> It is a common misconception that the remediation of an incident is relevant to whether the incident occurred in the first place. Whether or not SolarWinds addressed this vulnerability does not mitigate the fact that this was a fundamental

---

<sup>107</sup> As I discussed elsewhere, according to Mr. Brown, SolarWinds effectively made it possible for hackers to distribute malware directly to SolarWinds customers by disguising malware as a legitimate SolarWinds product. SW-SEC00407702–707 at 702. (Brown: “With that credential they could upload anything to downloads.solarwinds.com [...] In their POC [proof of concept] they uploaded a file to the site. I have made an assumption that this is our main download site since [we] needed to confirm the download site with on internal checksums [sic]. The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site.”) *See also* Graff Opening Report, ¶ 91.

<sup>108</sup> Graff Opening Report, ¶ 91. SW-SEC00407702–707 at 704 (“On 19 Nov 2019 PSIRT received a report from an external researcher about hardcoded credentials in one of [sic] publicly available Github repos.”).

<sup>109</sup> Quitugua Investigative Testimony, Vol. II, at 362:7-15. (“Q Are you aware of solarwinds123 being used as a password in other parts of the organization? A [...]. There may have been the possibility that in the lab environments, passwords such as, you know, weak passwords that were in use.”). Deposition of Timothy Brown, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 3, 2024 (“Brown Deposition”) at 120:14-15. (“A I’m not saying that [...] the password policy was followed a hundred percent of the time.”). *See also* Graff Opening Report, ¶¶ 133-134.

<sup>110</sup> As I discuss in Section III.B.2, Dr. Rattray conjured non-existing language in the Security Statement to argue that “the most sensible way to read this statement is that SolarWinds automatically required the use of complex passwords *where it was feasible to do so* [emphasis added].”

<sup>111</sup> Rattray Report, ¶ 177.

cybersecurity weakness—an opinion that Mr. Brown himself expressed to his colleagues after the incident was remediated.<sup>112</sup> This suggests to me systemic problems, which should not have existed in the first place if SolarWinds had followed the security practices asserted in the Security Statement.<sup>113</sup> Additionally, the bug bounty program is completely unrelated to the Security Statement, and the existence of such a program does not make up for SolarWinds’ lack of undertaking the security actions described in the Security Statement.

## VI. SOFTWARE DEVELOPMENT LIFECYCLE

49. In this section, I address why Dr. Rattray was incorrect in opining that my Opening Report did not show any systemic failure to follow the Software Development Lifecycle (“SDL”). Dr. Rattray did not dispute that the poor practices I discussed in my Opening Report existed during the Relevant Period. Instead, he focused on which part of the Security Statement the practices contradicted and which activities the Security Statement applied to. Dr. Rattray also failed to present evidence of threat modeling, which is a standard security practice within a secure development lifecycle, and would have been a fundamental element of the “security best practices” mandated by the company “across all development activities,” as claimed in the Security Statement.

### A. Dr. Rattray’s Statements Related to the Separation of Development and Production Environments Are Incorrect

50. When discussing the lack of separation between development and production environments at SolarWinds and its relation to the SDL, Dr. Rattray once again dismissed the

---

<sup>112</sup> SW-SEC00407702–707 at 702. (“This was managed and resolved quickly but *it did take place* [emphasis added] and a very weak password existed to access” the environment that “could have corrupted one of our downloads.”).

<sup>113</sup> Graff Opening Report, ¶ 92.

gravity of SolarWinds’ ongoing practice of developers working with billing data from production as a “one-off incident.”<sup>114</sup> I have already explained in **Section IV.A** why Dr. Rattray was mistaken in asserting that this was a “one-off incident” of little import. It is worth reiterating, however, that Chris Day, SolarWinds’ current CIO, assessed this issue as “a significant security [...] violation” that “needs to stop immediately” and that “under no circumstances” it should have happened.<sup>115</sup>

51. Dr. Rattray not only dismissed the importance of this particular event, but also asserted that the Security Statement’s provision regarding separate development and production environments “is an issue relating to the company’s network security, not its software development lifecycle.”<sup>116</sup>

52. I disagree. This statement relates to best practices pertaining both to network security and to software development. This is a software development concern because it relates to the behaviors and practices employed to develop software. In fact, within SolarWinds’ detailed version of the Security Statement, made available to customers upon request, the statement “SolarWinds maintains separate development and production environments[,]” was

---

<sup>114</sup> Rattray Report, ¶ 191.

<sup>115</sup> SW-SEC00254254–266 at 265. (From Chris Day, VP of Global DevOps and Technology Operations: “Hello – highlighted item [The developers are developing in Production] needs to stop immediately. Under no circumstances is development to be done in production. If that impacts deliverables please let August know. That is a significant security and Sox violation. As part of our ISO it also need to be filed as a non-conformity and reported.”).

<sup>116</sup> Rattray Report, ¶ 185. (“Mr. Graff starts by making an argument that does not even relate to SolarWinds’ software development lifecycle, i.e., to the steps that engineers follow in developing software. He instead challenges the Security Statement’s representation that ‘SolarWinds maintains separate development and production environments.’ That is an issue relating to the company’s network security, not its software development lifecycle—which is why it appears under the heading ‘Network Security’ in the Security Statement.”).



contained under both the Network Security sections *and* the Application Security – Software Development Lifecycle sections verbatim.<sup>117</sup>

53. The direction to maintain a separate development environment does not simply mean that such a development environment exists, it also necessarily requires that software development activities are restricted to that environment. If you are performing development activities inside a production environment, you have clearly failed to segregate development from production. This is a problem because, as I explained in my Opening Report, and as industry bodies (including NIST and the ISO) agree, without separating the development and production environments, organizations increase the risk of—among other things—“unauthorized access or changes to the operational environment.”<sup>118</sup>

54. Dr. Rattray did not dispute in his report that development activities occurred in the production environment during the Relevant Period (which is, in substance, what matters), and instead quibbled over which part of the Security Statement this poor practice contradicted.<sup>119</sup> Dr. Rattray’s statement that “all that was happening here was that developers were working *inside* [emphasis in original] the production environment” clearly described a problem, which

<sup>117</sup> SW-SEC00292763–781 (Detailed SolarWinds Security Statement dated May 2018, shared by Tim Brown via email on April 16, 2019), at 772 and 780.

<sup>118</sup> ISO, *ISO/IEC 27001:2013(E): Information Technology — Security Techniques — Information Security Management Systems — Requirements*, October 01, 2013 (“ISO/IEC 27001:2013(E)”), A.12.1.4. (“Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.”). *See also* NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 16, 2018 (“NIST Cybersecurity Framework”) at p. 33. (“PR.DS-7: The development and testing environment(s) are separate from the production environment[.]”). Graff Opening Report, ¶ 151.

<sup>119</sup> Rattray Report, ¶¶ 189-190. (“Instead, all that was happening here was that developers were working *inside* the production environment. They weren’t disabling the firewall between the production environment and exposing it to threats from the infrastructure in the development environment; they were simply logged into the production environment—with its more securely configured infrastructure—and testing a billing application on live data in that environment. Now, as I discussed earlier, this did pose a potential risk: The developers might accidentally modify the billing data, which, because it was live data, might cause inaccuracies in billing or financial reporting. But that risk has nothing to do with any network-security concern about failing to segregate the DEV and CORP environments.”).



was not and cannot be solved with firewalls, as Dr. Rattray suggested.<sup>120</sup> Indeed, firewalls did not separate the development and production activities occurring *within the same environment*, a behavior that directly contradicted the Security Statement’s broad assertion that “SolarWinds maintains separate development and production environments”<sup>121</sup> and that, as I explain in my Opening Report, creates significant cybersecurity risks for a company.<sup>122</sup>

**B. Dr. Rattray’s Statements Related to the Development of Internal Software Applications Are Flawed**

55. Reciting Mr. Brown’s deposition testimony,<sup>123</sup> Dr. Rattray opined that “[t]he Security Statement does not make any representations about the process SolarWinds followed in developing internal software applications that it used for its own business purposes.”<sup>124</sup> I disagree.<sup>125</sup> The Security Statement asserted that security testing is implemented “throughout the *entire* software development methodology” and that “security best practices are a mandated

---

<sup>120</sup> Rattray Report, ¶ 190.

<sup>121</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement).

<sup>122</sup> Graff Opening Report, ¶¶ 143, 152-153.

<sup>123</sup> Rattray Report, ¶ 195. Brown Deposition at 123:13-24, 271:7-14. (“Q. The first sentence states, ‘We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products.’ To your understanding, was that statement accurate when the security statement was published on the SolarWinds’ website? A. Yes, we had a -- a defined methodology to build products. We had defined groups for, uh, the major functions of product development, uh, and that our software is -- is designed, uh, designed for to be to increase resiliency and trustworthy of our product. [...] Q. So were the BizApps sold to customers or were they solely used within SolarWinds? A. Solely used within SolarWinds. Q. Were those developed pursuant -- pursuant to SolarWinds’ secure development lifecycle? A. Uh, they -- they were not products. So as the statement says, it’s for products. So products go through this cycle.”).

<sup>124</sup> Rattray Report, ¶ 194.

<sup>125</sup> I further disagree with Dr. Rattray’s assertion that “Mr. Graff ignores that, in discussing SolarWinds’ software development lifecycle, the Security Statement refers specifically to ‘our products’—a term that he himself used in his report to refer to software sold to SolarWinds’ customers.” Rattray Report, ¶ 197. I did not ignore it. In fact, I explained in my Opening Report precisely why I disagree with Mr. Brown’s (and now Dr. Rattray’s) statement that the Security Statement’s assertions about a software development lifecycle referred exclusively to products sold to customers. Graff Opening Report, Section IV.D.3.b.

aspect of *all* development activities.”<sup>126</sup> In my opinion, a reasonable reading of these statements would mean that software developed by the company, be it for internal or customer use, would be included under the rubric “all development activities.”

56. This would include OIP, which Dr. Rattray said was “not software that SolarWinds customers used; it resided on SolarWinds own network and was used by SolarWinds. [...] OIP was not a ‘component’ of the Orion software that ran on customer systems, nor was it otherwise ‘used’ by customers[:] OIP was an application that SolarWinds ran on its own server and that SolarWinds used for its own business purposes.”<sup>127</sup> However, Dr. Rattray ignored that SolarWinds’ failure to develop OIP according to its own secure development lifecycle (a fact he did not dispute) created a risk – which would not have been mitigated by the details of how OIP operated.

57. Dr. Rattray appeared to suggest in his report that this OIP-related risk was not significant and that I “misportray[] [it] as a major issue.”<sup>128</sup> Contrary to Dr. Rattray’s assertion, however, internal documents reveal that SolarWinds employees considered the vulnerabilities in the OIP server to be a major issue and advocated to bring it under the software development lifecycle. A June 2020 email exchange indicates that SolarWinds employees considered OIP to pose a significant risk to customers. For example, Tomas Vrabel, a Senior Architect at SolarWinds,<sup>129</sup> warned that

“OIP API is not authenticated so it can accept content for any user, API is exposed externally so everybody can access it. **If the OIP server is compromised, consequences can be disastrous** —

<sup>126</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

<sup>127</sup> Rattray Report, ¶ 199. Emphasis removed.

<sup>128</sup> Rattray Report, ¶ 204.

<sup>129</sup> SW-SEC00509572 at tab “Employee Listing 06-01-2020.”

ranging from simple XXE attacks or collection of customer credentials to attacks like **taking over all customer installations.**”<sup>130</sup> (Emphasis added.)

Later, Chris Erway, a Senior Director of Architecture at SolarWinds,<sup>131</sup> added:

“Oh, yikes, I often forget that on-prem[ises] Orion already has a SaaS [software as a service] endpoint open to the public Internet – OIP. **Sounds pretty important, I didn’t realize it’s possible an attacker could use it to take over all customer installations.**”<sup>132</sup> (Emphasis added.)

58. Dr. Rattray focused not on the OIP-related vulnerability itself, but rather SolarWinds’ response to the possibility of the vulnerability having been exploited.<sup>133</sup> This approach was incorrect. My Opening Report considered what this vulnerability reflected about SolarWinds’ software development process and how it related to the assertions made in the Security Statement. Put simply, how SolarWinds responded to an incident is not relevant to the question of whether SolarWinds employed the software development lifecycle best practices across all development activities, as it asserted in the Security Statement.<sup>134</sup>

<sup>130</sup> SW-SEC00000673–678 (Email from Tomas Vrabel on June 23, 2020) at 678.

<sup>131</sup> SW-SEC00509572 at tab “Employee Listing 06-01-2020.”

<sup>132</sup> SW-SEC00000673–678 (Email from Chris Erway on June 24, 2020) at 676.

<sup>133</sup> Rattray Report, ¶ 203. (“This is exactly what I would expect a well-functioning cybersecurity program to do in this scenario, where there was a specific indication of a threat actor targeting the OIP server as a potential entry vector into SolarWinds: aggressively investigate every possible weakness in the OIP server to ensure that it was adequately protected. As it turns out, the entire exercise was a fire drill, as SolarWinds found no signs of compromise on the OIP server, and, as was eventually learned, the incident did not actually involve any attempt to compromise the OIP server.”).

<sup>134</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement). (“Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities. Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments.”).

**C. Dr. Rattray’s Statements Related to Threat Modeling and Security Testing Are Incorrect**

59. The Security Statement asserts that:

**“Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities. Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments.”**<sup>135</sup> [emphasis added]

60. Dr. Rattray concluded that, because the Security Statement does not explicitly assert that SolarWinds practices threat modeling, it is improper to infer that the Security Statement indicates that it does.<sup>136</sup> In my opinion, this is incorrect. The Security Statement asserts plainly that SolarWinds *mandates security best practices*; and threat modeling is a fundamental standard security practice within a secure development lifecycle. This fact, which I also discussed in my Opening Report,<sup>137</sup> is recognized by many leading industry bodies, including OWASP,<sup>138</sup> NIST,<sup>139</sup> and Microsoft.<sup>140</sup> For example, the OWASP resource that Dr. Rattray cited in his report<sup>141</sup> states that “Microsoft [...] includes threat modeling as a key

<sup>135</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement).

<sup>136</sup> Rattray Report, ¶ 206. (“Regardless of whether Mr. Graff believes that threat modeling is a ‘standard security practice,’ the Security Statement did not make any open-ended statement that the company follows ‘all’ ‘standard security practices’[...] [...] The Security Statement instead specified which ‘standard security practices’ the company followed with respect to software development—namely, vulnerability testing, regression testing, penetration testing, and product security assessments.”).

<sup>137</sup> Graff Opening Report, ¶ 142.

<sup>138</sup> OWASP, “OWASP Threat Modeling Project,” <https://owasp.org/www-project-threat-model/#>.

<sup>139</sup> See, e.g., NIST, *NIST Special Publication 800-154: Guide to Data-Centric System Threat Modeling*, March 2016.

<sup>140</sup> See, e.g., Howard, Michael and Steve Lipner, *Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*, Microsoft Press, 2006, Chapter 9.

<sup>141</sup> Rattray Report, ¶ 207.

activity in their Security Development Lifecycle (SDL).”<sup>142</sup> Contrary to Dr. Rattray’s specious argument that I am “read[ing] representations into the Security Statement,”<sup>143</sup> the Security Statement explicitly stated that “[s]ecurity and security testing are *implemented* throughout the entire software development methodology [emphasis added].”<sup>144</sup> Yet, as I explained in my Opening Report, SolarWinds employees were aware that the company did not consistently engage in threat modeling.<sup>145</sup> Importantly, without threat modeling, companies and their customers may be open to significant cybersecurity risks that could be prevented otherwise.

61. While threat modeling can be achieved in different ways, security best practices require a structured approach to threat modeling that, at a minimum, should be performed at design time or during the design review. Indeed, the OWASP webpage that Dr. Rattray used as a source for opinions in his report explains that:

“A threat model is essentially a **structured** representation of all the information that affects the security of an application. [...] Threat modeling is a process for **capturing, organizing and analyzing** all of this information. Threat modeling **enables informed decision-making** about application security risk. In addition to producing a model, typical threat modeling efforts also produce **a prioritized list of security improvements to the concept, requirements, design, or implementation** [emphasis added].”<sup>146</sup>

62. In contrast, Dr. Rattray asserted in his report that “[t]hreat modeling’ is a loose term that can encompass *virtually any effort* [emphasis added] to anticipate and address potential

---

<sup>142</sup> OWASP, “OWASP Threat Modeling Project,” <https://owasp.org/www-project-threat-model/#>, at tab “Threat Modeling.”

<sup>143</sup> Rattray Report, ¶ 206.

<sup>144</sup> SW-SEC00466120–142 (SolarWinds’ Security Statement).

<sup>145</sup> Graff Opening Report, Section IV.D.3.

<sup>146</sup> OWASP, “OWASP Threat Modeling Project,” <https://owasp.org/www-project-threat-model/#>, at tab “Threat Modeling.”

security threats as part of the software design process.”<sup>147,148</sup> Dr. Rattray’s approach is not in line with threat modeling best practices described by leading industry bodies, as demonstrated by the OWASP quote above, as well as Microsoft, which pioneered the SDL process including threat modeling.<sup>149</sup>

63. To further support his opinion that SolarWinds was performing threat modeling during the Relevant Period, Dr. Rattray cited the deposition testimony of Mr. Kim and Mr. Colquitt.<sup>150</sup> Dr. Rattray, for example, recited Mr. Colquitt’s incorrect testimony that “threat modeling is ‘inherent’ in assessing and addressing security risks in software[,]” that “[t]hreat modeling can be done verbally, it can be done on a piece of paper, it can be done on a whiteboard or you can use a formal tool to produce that documentation[,]”<sup>151</sup> and that “the very fact that SolarWinds’ products ‘had security controls in them’ is by itself evidence of threat

<sup>147</sup> Rattray Report, ¶ 207. (“In any event, Mr. Graff ignores evidence in the record that SolarWinds did conduct threat modeling as part of its secure software development processes. ‘Threat modeling’ is a loose term that can encompass virtually any effort to anticipate and address potential security threats as part of the software design process. For example, the OWASP Foundation, a well-recognized authority on software security, defines threat modeling as essentially a process for asking the following four questions: [1] What are we working on? [2] What can go wrong? [3] What are we going to do about it? [4] Did we do a good job? As OWASP states, ‘[t]here are many methods or techniques which can be used to answer each of these questions,’ with ‘no ‘right’ way’ that one must use.”).

<sup>148</sup> Dr. Rattray attempts to also minimize my use of an internal SolarWinds document with an assessment stating that “[n]o threat modelling [sic] nor analysis is performed as part of any process (except MSP Backup Engineering).” Dr. Rattray speculated that “[t]he authors who wrote this assessment (who were not deposed) may have had in mind a *formalized* [emphasis in original] type of threat modeling that they wanted to be done, rather than meaning to say that no type of threat modeling was being done in any sense.” I note, however, that security best practices, as asserted in the Security Statement, require a *formalized* approach to threat modeling. *See* Rattray Report, ¶ 212.

<sup>149</sup> *See e.g.*, Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>. *See also*, Howard, Michael and Steve Lipner, *Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*, Microsoft Press, 2006, Chapter 9.

<sup>150</sup> Rattray Report, ¶ 208-209.

<sup>151</sup> Rattray Report, ¶ 208. (“Mr. Colquitt similarly explained at his deposition that threat modeling is ‘inherent’ in assessing and addressing security risks in software: ‘[W]hen I assess a particular requirement, I identify a risk and I mitigate that risk, that is threat modeling.’ As he stated, there is no one way to do this: ‘Threat modeling can be done verbally, it can be done on a piece of paper, it can be done on a whiteboard or you can use a formal tool to produce that documentation. There’s multiple ways to do this exercise.’”).

modeling, because ‘[t]hose security controls are the outputs of a threat model having taken place.’”<sup>152</sup>

64. In my opinion, Mr. Kim and Mr. Colquitt’s deposition testimony, that SolarWinds performed threat modeling during the Relevant Period, is not consistent with what is commonly understood as security best practices as it relates to threat modeling.<sup>153</sup> Put simply, the minimal and unstructured process described by Dr. Rattray, in my opinion, does not comport with the security best practices that SolarWinds asserted to follow in the Security Statement, and which are commonly implemented in the industry as part of software development lifecycles.<sup>154</sup>

65. Among the most important questions threat modeling attempts to answer—which Dr. Rattray acknowledges<sup>155</sup>—are: “[1] What are we working on? [2] What can go wrong? [3] What are we going to do about it?”.<sup>156</sup> These are all questions that, as a best practice, need to be evaluated and answered early on in the process of developing software, as they will substantially influence design, implementation, and testing (among other elements of

<sup>152</sup> Rattray Report, ¶ 209. (“Mr. Kim and Mr. Colquitt both testified that SolarWinds did threat modeling as part of the software development process, even if there was no one standardized way in which it would be done or documented. As Mr. Colquitt noted, the very fact that SolarWinds’ products ‘had security controls in them’ is by itself evidence of threat modeling, because ‘[t]hose security controls are the outputs of a threat model having taken place.’ Moreover, as Mr. Brown noted in his deposition testimony, SolarWinds had a dedicated architecture team in place, consisting of ‘very senior engineers,’ whose job it was to conduct ‘design reviews’ in order to ensure ‘that things were designed appropriately.’”).

<sup>153</sup> See, e.g., Deposition of Steven Colquitt, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 18, 2024 (“Colquitt Deposition”), at 65:16-23, 66:5-13, 165:10-12, 206:15-207:2; Deposition of Woong Joseph Kim, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 16, 2024 (“Deposition of Woong Joseph Kim”), at 148:12-24, 203:1-2.

<sup>154</sup> Dr. Rattray appears to state that “virtually any effort” to ask the four questions he quotes from OWASP represent a threat model (including simply “thinking about potential security risks and potential mitigations for them”). See Rattray Report, ¶ 207. See also, Rattray Report, ¶ 210. (“All of this evidence is consistent with the testimony of Mr. Kim and Mr. Colquitt that SolarWinds did threat modeling. Indeed, as Mr. Colquitt explained, it is hard not [emphasis removed] to do threat modeling in some form if security is being considered during the software development process—as it clearly was at SolarWinds—because consideration of security inherently involves thinking about potential security risks and potential mitigations for them.”).

<sup>155</sup> Rattray Report, ¶ 207.

<sup>156</sup> OWASP, “OWASP Threat Modeling Project,” <https://owasp.org/www-project-threat-model/#>, at tab “Main.”



development).<sup>157</sup> As a result, if SolarWinds had comported with security best practices as asserted in the Security Statement, I would have expected to see formal documentation from the Relevant Period showing that early on in the development process, typically at design time, SolarWinds considered, among other things, assets and trust relationships, as well as potential threat actors and entry points. As an illustration, Microsoft stated in its seminal 2006 SDL book that

“The main output of the threat-modeling process is a document (or documents) that describes background information about the application and defines the high-level application model, often by using data flow diagrams (DFDs); a list of assets that require protection; threats to the system ranked by risk; and, optionally, a list of mitigations. Relevant background information includes the following:

- **Use scenarios** Deployment configurations and broad customer uses
- **External dependencies** Products, components, or services the application or system relies on
- **Security assumptions** Assumptions you make about the security services offered by other components
- **External security notes** Information useful to your product’s end user or administrator to operate the system securely.”<sup>158</sup>

66. In my experience, it is industry best practice for software development companies to adopt formal written procedures for threat modeling. Moreover, it is also security best practice

<sup>157</sup> See, e.g., Howard, Michael and Steve Lipner, *Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*, Microsoft Press, 2006, p. 101. (“[W]hen performed correctly, threat modeling occurs early in the project lifecycle and can be used to find security design issues before code is committed. This can lead to significant cost savings because issues are resolved early in the development lifecycle.”).

<sup>158</sup> Howard, Michael and Steve Lipner, *Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*, Microsoft Press, 2006, p. 103. I also note that the OWASP resource that Dr. Rattray described a similar process. See OWASP, “OWASP Threat Modeling Project,” <https://owasp.org/www-project-threat-model/#>, at tab “Application Threat Modeling.”



for companies to produce analyses documenting the threat modeling exercise, identifying potential threat actors and how they typically operate in the environment in which the software will function (e.g., the techniques and potential attack vectors that have been observed by those threat actors), determining those threat actors' likely targets (e.g., some threat actors may pursue vulnerabilities in outward facing websites, while others tend to focus on attacking third-party vendors), and the software's so-called "attack surface" (i.e., the sum of vulnerabilities, pathways, or methods hackers can use to carry out a cyberattack),<sup>159</sup> among other elements.

67. I have seen no documentation showing that SolarWinds consistently engaged in threat modeling, which would have been a fundamental element of the "security best practices" mandated by the company "across all development activities," as claimed in the Security Statement. I note that Dr. Rattray provided no such evidence in his report either. Instead, Dr. Rattray pointed to a set of Final Security Reviews ("FSRs"),<sup>160</sup> which he described as documents "that engineering teams were required to prepare at the *last phase of the process, prior to [product's] release* [emphasis added]"<sup>161</sup> and that "contain numerous artifacts of security testing."<sup>162</sup> The FSRs I have reviewed do not contain a threat analysis (typically conducted prior to software development), where the threat modeler would anticipate and propose

---

<sup>159</sup> IBM, "What Is an Attack Surface?," June 28, 2022 <https://www.ibm.com/think/topics/attack-surface>. ("An organization's attack surface is the sum of vulnerabilities, pathways, or methods—sometimes called attack vectors—that hackers can use to gain unauthorized access to the network or sensitive data, or to carry out a cyberattack.")

<sup>160</sup> Rattray Report, ¶ 210.

<sup>161</sup> Rattray Report, ¶ 94. ("The most significant artifacts I have reviewed from SolarWinds' software development process, however, are 'Final Security Reviews' or 'FSRs' that engineering teams were required to prepare at the last phase of the process, prior to release. As Mr. Colquitt testified, this was a new form of documentation SolarWinds rolled out in early 2018, which engineering teams gradually adopted over the ensuing months. The FSRs were designed to pull together in one place various artifacts of security testing that were done in connection with a software release across different phases of the development process. The FSRs included sections for engineers to post links to tickets ('stories') in JIRA concerning security issues found and addressed through security testing, as well as places to post summaries of or links to the results of vulnerability scans and penetration tests.")

<sup>162</sup> Rattray Report, ¶ 95.

countermeasures to threats and vulnerabilities. That is, I have not seen documents describing, among other things, the key assets, trust relationships, potential threat actors and entry points. Instead, the FSRs generally contain an inconsistent hodge-podge of checklists of security-related activities. These reviews provide limited context to and information about whatever underlying security activities SolarWinds performed.<sup>163</sup>

68. Dr. Rattray contended that the fact that, for example, “some FSRs include documents specifically labeled ‘Threat Model’” and “[s]ome of the FSRs also include design reviews by the Architecture Team,” comprised conclusive evidence that SolarWinds performed threat modeling.<sup>164</sup> However, Dr. Rattray provided no analysis of the underlying material, *i.e.*, of the *contents* of those documents “labeled ‘Threat Model’” or resulting from the “design reviews by the Architecture Team.” Thus, Dr. Rattray merely speculated that the contents of these documents contain evidence that SolarWinds was performing threat modeling during the Relevant Period.

69. Moreover, the fact that the FSRs I have reviewed included disparate references to potential threat modeling activities is additional evidence that SolarWinds did not have a structured approach to threat modeling. Put simply, the select FSRs highlighted in Dr. Rattray’s

---

<sup>163</sup> Dr. Rattray also pointed to the FSRs that contained “summaries of or references to” Burpsuite reports as evidence of SolarWinds’ penetration testing activities. (Rattray Report, ¶ 95.) Contrary to Dr. Rattray’s characterization, I never claimed that SolarWinds “failed to do penetration testing[.]” (Rattray Report, ¶ 215.) Therefore, I did not need to provide “an example of any instance when penetration testing did not happen[.]” as he claims I failed to do. (Rattray Report, ¶ 214.) Instead, what I argued in my Opening Report is that in my opinion, if customers often found vulnerabilities that SolarWinds had missed before releasing its products, this should have alerted SolarWinds leadership that its own penetration testing was not following “security best practices” as asserted in the Security Statement. (Graff Opening Report, ¶ 188.)

<sup>164</sup> Rattray Report, ¶ 210. While Dr. Rattray states that “[s]ome of the FSRs also include design reviews by the Architecture Team,” Dr. Rattray also states that the FSRs include “links to design reviews done by the Architecture Team.” (Rattray Report, ¶ 95). I have not seen the content of those links and it is unclear whether Dr. Rattray has seen the content of these links either.

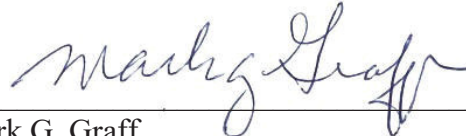
report do not comport with security best practices within the software development lifecycle, as asserted in the Security Statement.

## VII. DECLARATION

70. The foregoing rebuttal report, in addition to my Opening Report, represent my opinions to date on this matter. I reserve the right to supplement my reports and opinions should additional information become available.

\* \* \*

Signed on January 24, 2025, at Fayetteville, Arkansas.

  
\_\_\_\_\_  
Mark G. Graff

## **REBUTTAL APPENDIX A**

## **Additional Materials Considered for the Rebuttal Report**

### **Legal Documents**

Expert Report of Gregory Rattray, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, November 22, 2024.

Expert Report of Mark G. Graff, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 25, 2024.

### **Books**

Howard, Michael, and Steve Lipner, *Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*, Microsoft Press, 2006.

### **Public Documents**

Digital Realty Trust, Inc., SEC Form 10-K, filed December 31, 2023.

General Motors Financial Company, Inc., SEC Form 10-K, filed December 31, 2023.

IBM, “What Is an Attack Surface?,” June 28, 2022 <https://www.ibm.com/think/topics/attack-surface>, accessed January 21, 2025.

MITRE, “CAPEC-459: Creating a Rogue Certification Authority Certificate,” July 31, 2018, <https://capec.mitre.org/data/definitions/459.html>, accessed January 21, 2025.

NIST, *NIST Special Publication 800-154: Guide to Data-Centric System Threat Modeling*, March 2016.

OWASP, “OWASP Threat Modeling Project,” <https://owasp.org/www-project-threat-model/#>, accessed January 22, 2025.

Skywest, Inc., SEC Form 10-K, filed December 31, 2023.

Zetter, Kim, “Hackers Breached Adobe Server in Order to Sign Their Malware,” *Wired*, September 27, 2012, <https://www.wired.com/2012/09/adobe-digital-cert-hacked/>, accessed January 21, 2025.

### **Additional Bates-Stamped Documents Considered**

SW-SEC-SDNY\_00047306–00051840.

SW-SEC-SDNY\_00051843–00052673.

SW-SEC-SDNY\_00054914.

SW-SEC-SDNY\_00055010.

SW-SEC-SDNY\_00055077–00055078.

SW-SEC-SDNY\_00055088–00055091.

SW-SEC-SDNY\_00055103–00055108.

SW-SEC-SDNY\_00055115–00055130.

SW-SEC-SDNY\_00055149–00055153.

SW-SEC-SDNY\_00055163–00055167.

SW-SEC-SDNY\_00055172–00055176.

SW-SEC-SDNY\_00055178–00055181.

SW-SEC-SDNY\_00055186-00055194.  
SW-SEC-SDNY\_00055235-00055256.  
SW-SEC-SDNY\_00055276-00055281.  
SW-SEC-SDNY\_00055301-00055305.  
SW-SEC-SDNY\_00055443-00193099.